2. The difference between the two types of vulnerability and their score.

Good question! Here's a breakdown of the **two main types of vulnerabilities** and how their severity is scored.

Types of Vulnerabilities & Their Scoring

1. Software Vulnerabilities

These are weaknesses in **software code**, applications, or systems that attackers can exploit.

Examples:

- **Buffer Overflow:** Overloading memory to execute arbitrary code.
- **SQL Injection (SQLi):** Manipulating database queries to extract or modify data.
- **Cross-Site Scripting (XSS):** Injecting malicious JavaScript into web pages.
- **Remote Code Execution (RCE):** Running commands remotely on a compromised system.

Scoring: CVSS (Common Vulnerability Scoring System)

CVSS is the industry standard for measuring vulnerability severity, scored from **0 to 10**:

- **Low (0.1 - 3.9)** → Minimal impact, difficult to exploit.
- **Medium (4.0 - 6.9)** → Limited impact, requires some skill.
- **High (7.0 - 8.9)** → Significant impact, easier to exploit.
- **Critical (9.0 - 10.0)** → Severe impact, easily exploitable (e.g., RCE).

🔹 **Example CVE Score:**

- **CVE-2021-44228 (Log4Shell)**: **10.0 (Critical)** → Remote Code Execution.

2. Misconfiguration Vulnerabilities

These result from **incorrect system settings** rather than software flaws.

Examples:

- **Default Credentials:** Admin/admin left unchanged.
- **Exposed Services:** Open SSH, FTP, or SMB ports.
- **Weak Permissions:** `chmod 777` on sensitive files.

- **Cloud Misconfigurations:** AWS S3 bucket open to the public.

Scoring: DREAD or STRIDE (Risk Assessment Models)

DREAD measures impact based on:

- **D**amage potential
- **R**eproducibility
- **E**xploitability
- **A**ffected users
- **D**iscoverability

◆ Example: **Exposed admin panel (no auth)**

- **DREAD Score:** High (easy to exploit, affects all users).

Key Difference

Type	Root Cause	Example	Scoring Method
Software Vulnerabilities	Coding flaws	SQLi, XSS, RCE	**CVSS (0-10)**
Misconfigurations	Human error / bad setup	Default passwords, open S3 buckets	**DREAD/STRIDE**

For **real-world pentesting**, **both types** must be checked, but **software vulnerabilities** are more likely to have **CVE scores** because they exist in software that many users share.